3Г

УДК 004.49

Е.А. Гришко, Ю.К. Орлов
Донецкий национальный технический университет, г. Донецк, Украина
Украина, 83000, г. Донецк, ул. Артема, 58

Система управления автоматическим распознаванием реального пользователя и компьютерной программы

E.A. Grishko, Ju.K. Orlov
Donetsk National Technical University, Donetsk, Ukraine
Ukraine, 83000, c Donetsk, Artema st., 58

The Control System of Automatic Recognition of the Actual User and Computer Program

К.А. Гришко, Ю.К. Орлов
Донецький національний технічний університет, м. Донецьк, Україна
Україна, 83000, м. Донецьк, вул. Артема, 58

Система управління автоматичним розпізнаванням реального користувача і комп’ютерної програми

В данной статье рассмотрена немаловажная проблема, которая возникла около пятнадцати лет назад – бот-сети (ботнеты, зомби-сети) и о возможном способе борьбы с этой проблемой, которую до сих пор очень сильно недооценивают до тех пор, пока не происходит утечка ценной информации с фирмы, не пропадают деньги с банковских карточек и прочие неприятности. Предложен для рассмотрения алгоритм системы управления автоматическим распознаванием реального пользователя и компьютерной программы.
Ключевые слова: бот-сеть, бот, зомби-сети, кража информации, кибершантаж, алгоритм.

In this paper the major problem that emerged about a decade ago - the botnet (botnets, zombie networks) and a possible way to deal with this problem, which is still very much overlooked as long as the leakage of valuable information with the firm, not lost money with bank cards and other troubles. Proposed an algorithm to address management system of automatic recognition of the actual user and the computer program.
Key words: botnet, bot, botnet, data theft, cyber blackmail, algorithm.

У даній статті розглянута важлива проблема, яка виникла близько п’ятнадцяти років тому – бот-мережі (ботнети, зомбі-мережі) та про можливий спосіб боротьби з цією проблемою, яку досі дуже сильно недооцінюють до тих пір, поки не відбувається витік цінної інформації з фірми, не пропадають гроші з банківських карток та інші неприємності. Запропонований для розгляду алгоритм системи управління автоматичного розпізнавання реального користувача і комп’ютерної програми.
Ключові слова: бот-мережа, бот, зомбі-мережі, крадіжка інформації, кібер-шантаж, алгоритм.

Введение

Бот-сеть (англ. *botnet* от *robot* и *network*) – это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами – автономным программным

обеспечением. Простейшая структура ботнета представлена на рис. 1. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на компьютере жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов заражённого компьютера. Обычно используются для рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании [2].

Бот-сеть является одним из прекрасных вариантов кибероружия с большими вычислительными возможностями, а также является замечательным способом анонимно заработать деньги. Организатор данной сети может управлять зараженными компьютерами в сети из любой точки планеты, при этом, фактически не рискуя быть обнаруженным. Владельцы своих компьютеров зачастую не подозревают о том, что они заражены и используются злоумышленниками, находятся под контролем третьих лиц. Такие зомби-машины входят в многомиллионные бот-сети.

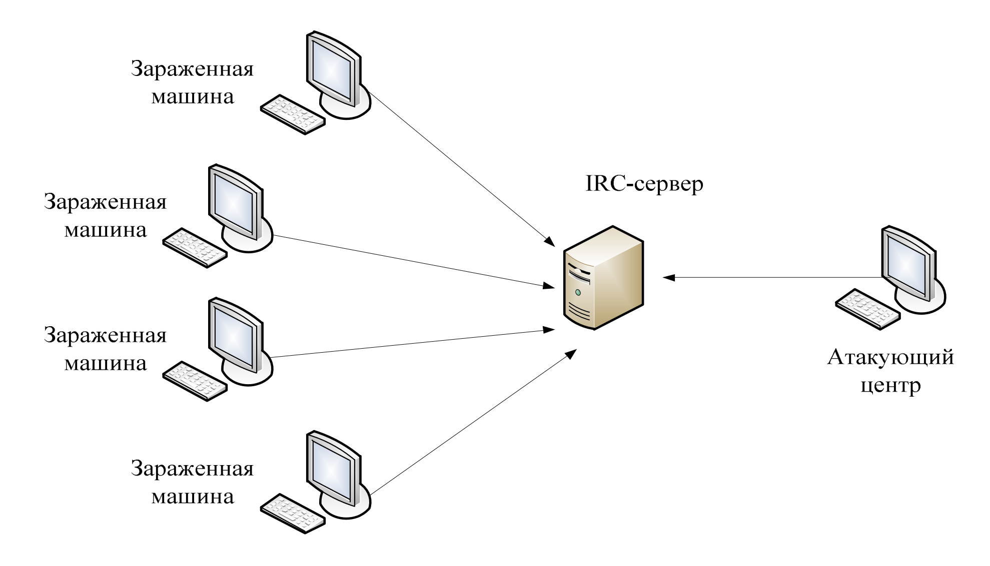


Рисунок 1 – Простая структура бот-сети

Ботнет может использоваться для самых разнообразных целей [1]: от обычной рассылки спама до атак на государственные сети. Коротко рассмотрим варианты использования бот-сетей:

1) рассылка спама. По подсчетам экспертов приблизительно 80% спама рассылается как раз при помощи бот-сетей. Среднестатистический спамер зарабатывает приблизительно 50 – 100 тысяч долларов в год на таких сетях. Бот-сети, предназначенные для рассылки спама, также могут собирать адреса электронной почты на зараженных машинах;

2) кибершантаж. Один из самых широко применяемых способов использования ботнета – проведение широкомасштабных DDoS-атак (от англ. *Distributed Denial of Service* – распределённая атака типа «отказ в обслуживании»). В ходе такой атаки с зомби-компьютеров на сервер посылается большой поток ложных запросов до тех пор, пока сервер не будет перегружен и станет не доступен пользователям, после чего владельцы бот-сети требуют выкуп за остановку атаки на сервер. Так как удачное ведение современного бизнеса не возможно без работы в интернете, владельцы сайта быстрее согласятся выплатить выкуп, чем обратятся в правоохранительные органы;

3) анонимный доступ в Сеть. Данный вариант использования бот-сети позволяет злоумышленникам от имени зараженных компьютеров осуществлять взлом сайтов, кражу денег с банковских счетов и т.д;

4) продажа и аренда бот-сетей. При помощи такого варианта владельцы бот-сетей также нелегально могут зарабатывать деньги;

5) фишинг (англ. *phishing*, от *fishing* – рыбная ловля, выуживание – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям). Бот-сеть позволяет фишерам быстро менять адрес фишинговой страницы, используя зараженные машины в качестве прокси-серверов, и при этом скрывать реальный адрес страницы;

6) кража конфиденциальных данных. Данный вид использования бот-сети позволяет красть всевозможные данные пользователей, которые потом перепродаются или используются для массового заражения веб-страниц с целью расширения бот-сети.

Целью данной работы является разработка алгоритма системы управления автоматическим распознаванием реального пользователя и компьютерной программы, который направлен на борьбу с бот-сетями.

Алгоритмы системы управления автоматическим распознаванием реального пользователя и компьютерной программы

Система управления автоматическим распознаванием реального пользователя и компьютерной программы предназначена для того, чтобы избежать кражи, потери информации, потери финансов и имиджа фирмы, а также многих других неприятных факторов. Структура данной системы представлена на рис. 2, где рассматривается вариант атаки сети ботнетом. При входе сигнала ***x*** в систему управления происходит одновременный мониторинг сети Internet и компьютера (управляющее устройство) при помощи программного обеспечения и технических средств контроля (исполнительный механизм), которые анализируют входной сигнал. Обнаружение атаки ботнета (объект управления) этими системами влечет за собой сигнализацию программными и техническими средствами, блокировку ботов, а затем поиск и блокировку центра ботнета.

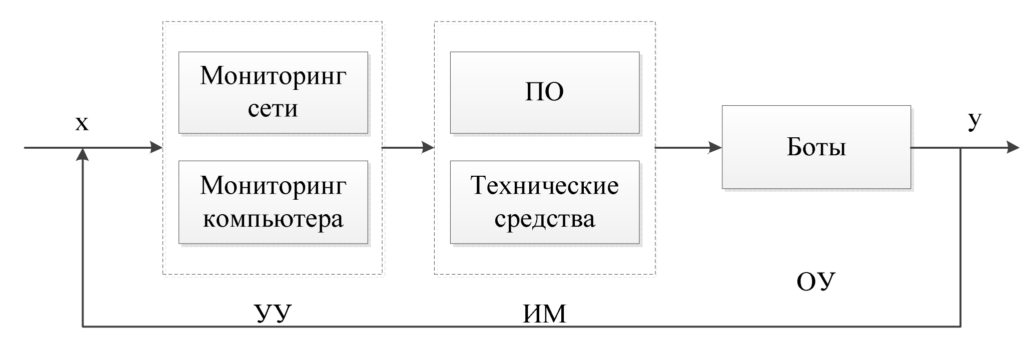


Рисунок 2 – Система управления автоматическим распознаванием реального пользователя и компьютерной программы

Система управления автоматическим распознаванием реального пользователя и компьютерной программы осуществляет двухуровневую защиту: с одной стороны на программном и техническом уровне, а с другой – мониторинг сети Интернет и рабочих машин с целью дальнейшего обнаружения и частичной или полной ликвидации бот-сети.

На рис. 3 представлен алгоритм работы предложенной системы.

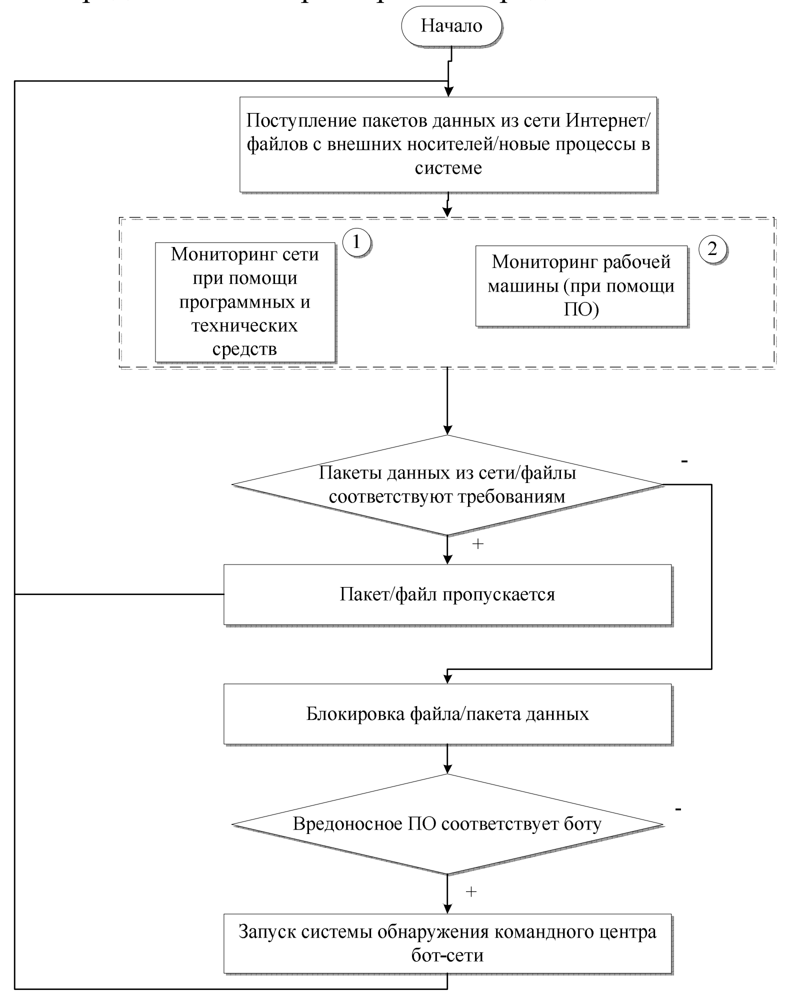


Рисунок 3 – Алгоритм работы системы управления автоматическим распознаванием реального пользователя и компьютерной программы

Рассмотрим более подробно данный алгоритм, начиная с алгоритма мониторинга рабочей машины (блок 2 на рис. 2) в двух случаях:

1) появление нового или измененного файла (рис. 4);

2) начало работы нового процесса (и этот процесс не был включен администратором системы в список разрешенных) (рис. 5).

Кроме существующих составляющих для этой системы предлагаются алгоритмы работы вспомогательных подсистем, которые позволят не только максимально возможно защитить работы организации (сайта), но и обнаружить источник негативного воздействия, а именно:

1) алгоритм для программного обеспечения, которое будет взаимодействовать с аппаратными средствами для сбора и анализа статистики входного траффика;

2) алгоритм для системы обнаружения командного центра бот-сети.

Обнаружение бот-сетей в первую очередь основано на анализе сетевого трафика. Совокупная информация об аномальных изменениях объемов входящего и выходящего трафика дает четкую картину о попытках нарушить работу, осуществить кражу информации и прочих воздействий на систему. Следовательно, алгоритм для сбора и анализа статистки входного трафика является важной составляющей всей системы.

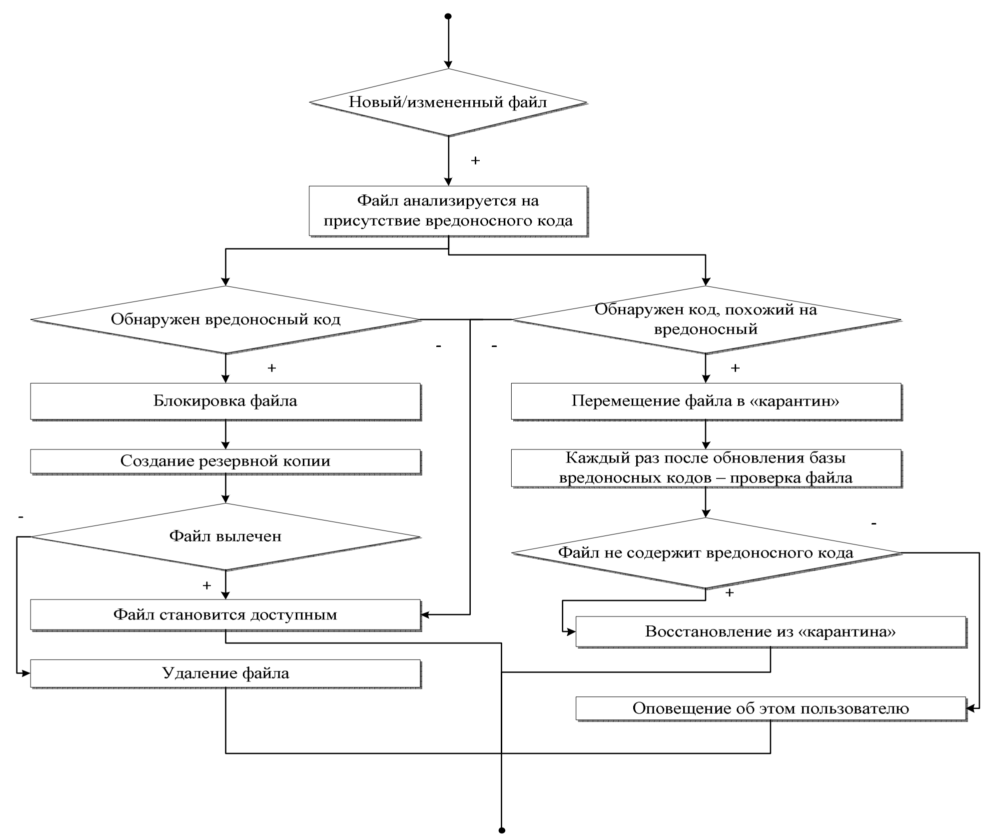


Рисунок 4 – Алгоритм мониторинга рабочей машины (в случае появления нового или измененного файла)



Рисунок 5 – Алгоритм работы мониторинга рабочей машины (в случае появления нового процесса)

Нейтрализация источника негативного воздействия на работу организации так же является немаловажной задачей, потому что попытки нарушения работы могут быть неоднократными, а на борьбу с действием бот-сети требуются много ресурсов и времени. Алгоритм системы обнаружения командного центра бот-сети представлен на рис. 6.

Данный метод обнаружения основан на том, что хост может находиться в одном из трёх состояний – либо легитимный IRC-клиент, либо бот, находящийся в состоянии ожидания команды, либо бот в состоянии атаки. Каждому из этих состояний соответствуют специфические значения средней длины пакета и частоты пересылки пакетов.

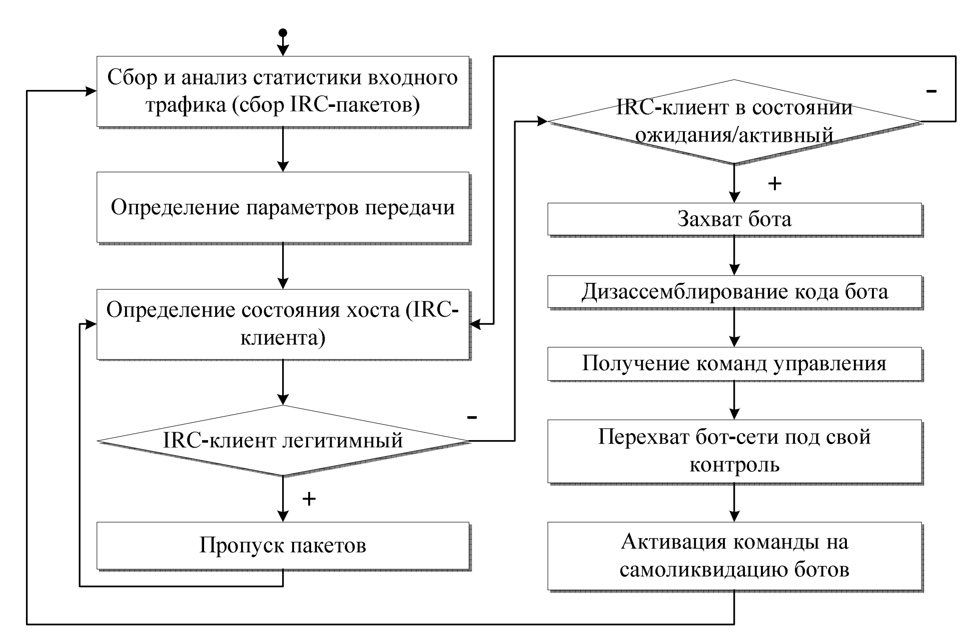


Рисунок 6 – Алгоритм обнаружения командного центра бот-сети

Выводы

Анализируя сегодняшнюю ситуацию развития кибер-преступности, можно прийти к выводам, что бот-сети являются одной из самых доходных сфер, а также, что злоумышленники вряд ли сами откажутся от подобного вида заработков, и, в свою очередь, вряд ли исчезнет конкуренция в сфере бизнеса, где сохранность информации и стабильность работы веб-сайтов является залогом успешного функционирования предприятий и фирм, а также государственных сетей. Хотя эксперты и предупреждают об опасности, которую несут развитие бот-сетей, большинство владельцев бизнеса, государство отказываются предпринимать какие-либо меры по защите от них до тех пор, пока не сталкиваются с подобной проблемой, а зомби-сети все продолжают и продолжают развиваться.

В результате проведенной работы был разработан алгоритм системы управления автоматическим распознаванием реального пользователя и компьютерной программы. Дальнейшие исследования будут направлены на моделирование данной системы для изучения эффективности алгоритма.

Литература

1. Официальный документ Cisco, Ботнет : новый характер угроз. – Cisco Systems, Inc, 2008. – 9 с. [Электронный ресурс] – Режим доступа : http://www.cisco.com/web/RU/downloads/Botnets.pdf.
2. Богданова, И.Ф. Информационная безопасность: классификация компьютерных угроз / И.Ф. Богданова // Интернет и современное общество : труды XI Всероссийской объединенной конференции (28 – 30 октября 2008 г., Санкт-Петербург). – СПб. : Факультет филологии и искусств СПбГУ, 2008. – С. 27-29 [Электронный ресурс]. – Режим доступа : http://conf.infosoc.ru/2008/pdf_HI/BogdanovaN.pdf

Literatura

1. Official document Cisco, Botnet: the new nature of the threats, Cisco Systems, Inc, 2008, 9 p. – URL: http://www.cisco.com/web/RU/downloads/Botnets.pdf.
2. Bogdanova, I.F Information security: classification of computer threats / IF Bogdanov / / Internet and Modern Society: Proceedings of the XI All-Russian Joint Conference (October 28-30, 2008, St. Petersburg). - St.: Faculty of Philology and Arts, St. Petersburg State University, 2008. – S. 27-29. – URL: http://conf.infosoc.ru/2008/pdf_HI/BogdanovaN.pdf

RESUME

E.A. Grishko, Ju.K. Orlov

The Control System of Automatic Recognition of the Actual User And Computer Program

In this paper the major problem that has arisen about fifteen years ago – botnets (botnets, zombie networks) and a possible way to deal with this problem, which is still very much overlooked as long as the leakage of valuable information with the firm, not lost money with bank cards and other troubles. We propose an algorithm to address management automatic recognition of the real user and a computer program.

Analyzing the current situation of cyber-crime, it can be concluded that the botnet is one of the most profitable areas, as well as that the attackers themselves hardly give up this type of earnings and, in turn, is likely to disappear in the competition business, where the security of information and the stability of the web is the key to the success of companies and enterprises, as well as public networks. While the experts are warning of the dangers posed by the development of botnets, most business owners, the government refused to take any steps to protect them as long as do not face the same problem, but the zombie network goes on and continue to develop.

As a result of this work has been developed algorithm control automatic recognition of the real user and a computer program. Further research will focus on modeling the system to study the effectiveness of the algorithm.

Статья поступила в редакцию 05.04.2013.